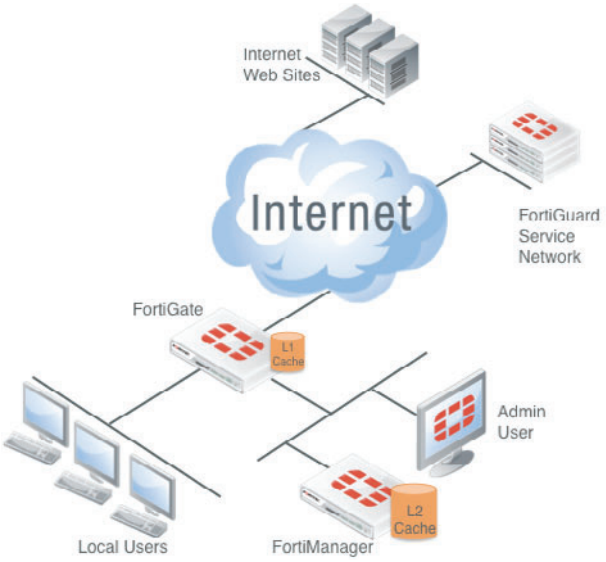
Web Filtering

FortiOS combines sophisticated filtering capabilities together with a powerful policy engine to create a high performance and flexible web content filtering solution

Cloud Based Model with FortiGuard Web Filtering Service

Fortinet provides an innovative approach to HTTP and HTTPS web filtering technology combining the advantages of a cloud based service offering with layered response caching. The multiple FortiGuard data centers around the world hold the entire categorized URL database and receive rating requests from customer FortiGate units triggered by browser based URL requests. These rating requests are responded to with the categories stored for specific URLs, the requesting FortiGate unit then uses its own local profile configuration to determine what action is appropriate to the category, such as: blocking, monitoring, allowing the page, displaying a warning, or requiring authentication to view the page.



Avoiding Cloud Latency

The question most asked when reviewing this architecture is the latency associated with the rating request. Fortinet has developed a lightweight query analogous to a DNS lookup. From an end-user perspective the delay introduced by the rating query is similar to the delay introduced by the DNS lookup, unperceivable in the majority of cases.

To maintain this low latency response time FortiGate units are constantly monitoring the performance of the FortiGuard URL rating service ensuring the next query is always sent to the fastest responding FortiGuard server. This latency optimization algorithm uses the geographic location of the FortiGate unit and FortiGuard servers, time zone, server load and real time response data to test queries and guarantee that minimum latency is always achieved.

Local Rating Cache

Rating responses are also cached directly in FortiGate unit memory so that ratings for frequently used sites can be retrieved directly from the cache, reducing the number of requests to the FortiGuard network. Caching URLs in memory makes URL lookups almost instantaneous while only using a very small amount of system memory.

FortiManager FortiGuard Database

An appropriately licensed FortiManager appliance can be synchronized to the FortiGuard network and as such be used in the same way to as the FortiGuard network for managed FortiGate devices. This can further reduce any latency associated with the round trip time for individual rating requests whilst at the same time ensuring complete database coverage. Consider the combination of a LAN attached FortiGate cluster and FortiManager combination with the potential to handle tens of thousands of requests per second.

FortiGuard Web Filtering Database

The database currently rates more than 104 million sites covering billions of URLs with each site able to be rated in multiple categories and data classes. With support for 70 languages the FortiGuard database provides a truly international service.For more information of the database, and to perform real time queries on the current database you can go to *http://www.fortiguard.com/webfiltering/webfiltering.html*

Enabling FortiGate Web Filtering

Fortinet's development team has ensured that providing this powerful filtering capability is as simple as possible. All FortiGate units ship with default web filter profiles designed to be useful for most organizations. Assuming the FortiGuard Web Filtering service is active (which can be easily verified form the Web UI) the administrator can enable web filtering by adding a default Web Filter profile to a security policy that accepts web traffic.

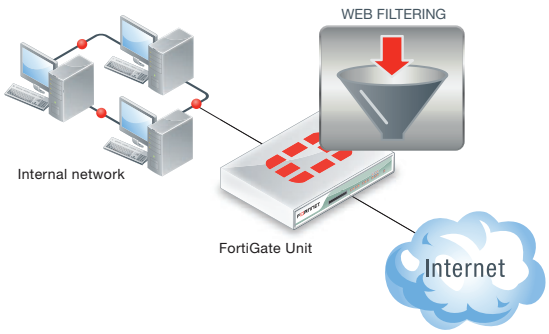
Customization of URL Categories

With the basic default protection in place administrators can customize Web Filtering by changing a default Web Filtering profile or by adding new custom Web Filtering profiles. This customization allows the selection of different web filtering modes, specific combinations of allowed, blocked or monitoring categories appropriate to any environment. In addition administrators can configure advanced features and populate local categories or place specific URLs in existing categories should the FortiGuard rating not be in agreement with an organization's policies and practices.

A Choice of Web Filtering technologies

FortiGate web filtering can operate in three modes. Each mode has strengths and weaknesses and all three can be active at the same time on different traffic streams.

Proxy-based web filtering uses a proxy to assemble and analyze web content as it passes through the FortiGate unit. If a page is blocked the proxy can replace the blocked page with a customizable web page informing users that the page is blocked. Proxy-based web filtering is the most feature rich mode, supporting many advanced filters including web content filtering that analyzes web page content according to your custom requirements, Java applet filtering and blocking invalid URLs.



Flow-based web filtering uses the FortiOS IPS engine to filter web content packets as they pass through the FortiGate unit without any buffering. Flow-based inspection does not use a proxy, so inspected packets are not proxied and altered by the FortiGate unit. Flow-based inspection does not support as many advanced features as proxy-based web filtering.

DNS web filtering employs DNS lookups to the FortiGuard DNS service to get web page ratings. Proxying or packet inspection is not required as the filtering is done as part of the DNS lookup and web pages can be blocked or redirected to a web filter block page before the HTTP session starts. DNS web filtering supports a limited number of advanced features.

Web Filtering Overrides

In some environments, especially in the education arena, access is blocked to certain categories but a user with additional authentication credentials may wish to override the block (teacher/student, adult education). The override feature allows a site that is otherwise blocked by the web filter profile to be unblocked after an additional layer of authentication has taken place.

User Identity Based Access Control

Having a single web filtering profile is seldom appropriate for an entire organization. Different groups of users often require varying levels of access that can change during the day. Typical examples include:

- Restricting access to social networking sites during core business times
- Imposing special restrictions on guest users access
- Limiting customer facing employee access

These scenarios require the end user to authenticate with the FortiGate unit to select the correct web profile to apply to each user's traffic. To ensure a completely flexible approach, a number of options are available to achieve end user identification:

- Local User Groups, with optional remote LDAP, RADIUS or TACACS+ databases
- Certificate based authentication, Two-factor authentication
- Temporary guest accounts, NTLM Authentication
- Directory Service, Windows and Citrix-based single sign on (SSO)

Device Identity Based Access Control

FortiOS device identity access control adds an additional layer of control by providing the ability to associate web filtering profiles with device types. Typical examples include:

- Restricting mobile phone access to social networking and gaming sites during office hours
- Imposing special restrictions on guest devices such as mobile phones or tablets used by visitors

Device identification can detect device types and impose restrictions completely transparently to the device user. Device types are identified by the FortiGate unit with no user authentication or identification required.

RADIUS SSO Authentication Extension

A RADIUS attribute value can be associated with a web filter profile and a RADIUS user profile, allowing FortiOS to apply different web filtering profiles to different users based on how they authenticate with an organization's RADIUS server. Authentication with the FortiGate unit is not required once the user has authenticated with the RADIUS server.

Consider the scenario where a user has been identified as a residential customer, it may be desirable to provide differing levels of service to users within the home. This residential parental control can also be provided to users even though they share a common IP address into the service provider network.

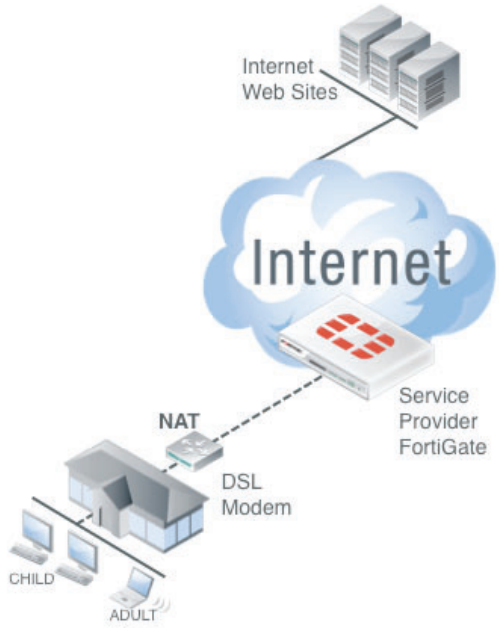


Image Rating

Where sites contain multiple images, sometimes from different websites it is a feature of FortiOS to allow these images to be separately rated to prevent inappropriate content being displayed. Images from blocked categories will not be displayed in the user's browser.

Safe Search and Search Engine Keyword Enforcement

Popular search engines include the ability to perform image searches, and display thumbnail image results. FortiOS provides a safe search option that enforces safe search mode for many popular search engines to limit the displayed results to content considered safe according to that search engine's standards.

YouTube Education Filter

YouTube for Schools (*http://www.youtube.com/schools*) limits access to educational YouTube content. If an organization has a YouTube for Schools account they can enter their account ID directly into their FortiGate web filtering profiles to apply their YouTube education filter to all YouTube traffic right from the FortiGate unit.

Web Filtering Quotas

Quotas can limit the amount of time spent viewing or the amount of data that can be downloaded from web sites according to their FortiGuard web filtering category. With quotas enabled it would be possible to, for example, limit access to gaming sites for two hours per day or limit the amount of data downloaded from streaming media sites. Quotas are set per web filter profile, accumulate over a 24 hour period, and reset at the end of the day.

Web Usage

Top Allowed Websites by Requests

Website	Requests
static.atm.youku.com	9
www.tudou.com	6
i3.tdimg.com	4
www.srh.noaa.gov	4
ad-g.doubleclick.net	3
ad.doubleclick.net	3
css.tudouui.com	3
i2.tdimg.com	3
i4.tdimg.com	3
googlesyndication.com	3

Replacement Pages

When a site is blocked a fully customizable replacement page can be sent in its place. These replacement pages are stored on the FortiGate unit and can be customized by FortiGuard category to include corporate branding (logos etc), provide details on the category of site blocked, references to any corporate policies, details on how to apply for override privileges or a simple 'site blocked' notification.

Top Websites by Bandwidth

Website	Bandwidth (Sent / Received)
windowsupdate.com	35.9 MB
www.bestbuy.ca	1.6 MB
windowsupdate.com	1011.8 KB
i4.tdimg.com	474.9 KB
www.youku.com	447.8 KB
i3.tdimg.com	377.4 KB
www.themarker.com	347.4 KB
i2.tdimg.com	281.6 KB
static.atm.youku.com	231.8 KB
www.youtube.com	198.7 KB

HTTPS Deep Scanning

HTTPS deep scanning provides FortiGuard web filtering of encrypted HTTPS sessions. HTTPS deep scanning performance is enhanced by leveraging FortiASIC HTTPS hardware acceleration. HTTPS deep scanning respects user's privacy by optionally not scanning banking, health care and personal privacy sessions.

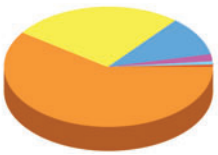
Reporting and client reputation

FortiGate units and the FortiCloud remote logging and reporting service generate daily security analysis reports that contain detailed information about website usage, blocked websites and other webfiltering-related output. Default reports are available that can be extended and customized as required. Reports at a username level can also be generated and user information can be provided directly from Microsoft Active Directory or Citrix environments.

To provide a consolidated report from multiple FortiGate devices a FortiAnalyzer appliance can be added to the solution allow a consolidated report to be produced for groups of FortiGate devices.

The client reputation feature can also be used for quick access to data about current web activity. Client reputation reports on and provides information about blocked URLs, visits to high-risk websites, visits to potentially liable sites, visits to adult/mature content, and visits to bandwidth consuming sites.

Top Web Streaming Websites by Bandwidth



%	Website	Bandwidth (Sent / Received)
59.7%	www.youku.com	458.5 K
26.5%	www.youtube.com	203.5 K
10.6%	www.tudou.com	81.2 K
0.7%	t.lstat.youku.com	5.5 K
0.6%	stat.tudou.com	4.8 K
2.0%	others	15.0 K